UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF NEW YORK

CALVIN CHENG, **Plaintiff,** **– against –** **T-MOBILE USA, INC.,** **Defendant.**	**Case No.: _____** **COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff CALVIN CHENG ("**Plaintiff**") by and through his attorneys, WILSON & CHAN, LLP, upon information and belief, complain and allege against **Defendant T-MOBILE USA, INC.** ("**T-Mobile**") as follows:

NATURE OF THE CASE

1. This action arises out of T-Mobile's systemic and repeated failures to protect and safeguard its customers' highly sensitive personal and financial information against common, widely reported, and foreseeable attempts to illegally obtain such information.

2. As a result of T-Mobile's gross negligence in protecting customer information, including its negligent hiring and supervision of customer support, technical, and administrative personnel and its violations of Federal laws designed to protect wireless service consumers, Plaintiff lost in excess of $750,000 in cryptocurrency due to an account takeover scheme (also

known as "SIM-swapping") which could not have occurred but for T-Mobile's negligent practices and its repeated failure to adhere to federal and state law.

3. T-Mobile is one of the nation's largest wireless carriers, having recently merged with Sprint and is governed by numerous federal statutes, including the Federal Communications Act (FCA).

4. T-Mobile regularly holds itself out as a secure custodian of customer data, including customer financial and personal information.

5. T-Mobile maintained in January 2021 that is used a "variety of administrative, technical, procedural, contractual, and physical security measures" to protect customer data against "accidental, unlawful, or unauthorized destruction, loss, alteration, access, disclosure, or use while it is under our control."[1]

6. Since that time, however, T-Mobile no longer claims to use "procedural" security measures nor does it any longer claim the safety measures it does use can protect customer data against "accidental, unlawful, or unauthorized destruction, loss, alteration, access, disclosure, or use while it is under our control."[2]

---

[1] Formerly available at https://www.t-mobile.com/privacy-center/our-practices/privacy-policy (last accessed Jan. 27, 2021).

[2] Available at https://www.t-mobile.com/privacy-center/our-practices/privacy-policy (last accessed May 15, 2022), stating, instead:

"We use administrative, technical, contractual, and physical safeguards designed to protect your data. For example, when you contact us by phone or visit us in our stores, we have procedures in place to make sure that only the primary account holder or authorized users have access.

7. Instead, it has simply issued a blanket statement that T-Mobile "can't guarantee our safeguards will prevent every unauthorized attempt to access, use, or disclose personal data."[3]

8. Moreover, as late as January 2021, T-Mobile stated that it maintained "authentication procedures when [customers] contact us by phone or in retail locations to help ensure that access is provided only to the primary account holder or authorized users of the account."[4]

9. As of May 2022, T-Mobile no longer includes such language in its Privacy Policy.[5]

10. All of these changes to its Privacy Policy, upon information and belief, serve as a powerful admission that T-Mobile has a real, ongoing, and devastating data security problem involving the loss, misuse, and abuse of millions of its customers' private data.

11. As T-Mobile is well-aware, SIM-swapping and other forms of account takeover fraud have been widely reported in the press and by government regulators, including the Federal Trade Commission (FTC) and the Federal Communications Commission (FCC), as well as by academic research teams.

We can't guarantee our safeguards will prevent every unauthorized attempt to access, use, or disclose personal data. Be sure to use a strong password to access your information and not one you use for other services. You should also use multi-factor authentication where possible."

[3] Id.

[4] Formerly available at https://www.t-mobile.com/privacy-center/our-practices/privacy-policy (last accessed Jan. 27, 2021).

[5] Available at https://www.t-mobile.com/privacy-center/our-practices/privacy-policy (last accessed May 15, 2022).

12. Account takeover schemes involve criminals and fraudsters gaining access to or "hijacking" customer wireless accounts, which often include sensitive personal and financial information, to induce third parties to conduct transactions with individuals they believe to be legitimate or known to them.

13. One of the most damaging and pervasive forms of account takeover fraud is "SIM-swapping" whereby a criminal third-party convinces a wireless carrier like T-Mobile to transfer access to one of its legitimate customers' cellular phone number from the legitimate customer's registered SIM-card – a small portable chip that houses identification information connecting an account to the wireless carrier's network[6] – to a SIM-card controlled by the criminal third-party.

14. This sort of account takeover is not an isolated criminal act, *per se*, as it requires the wireless carrier's active involvement to swap the SIM to an unauthorized person's phone.

15. As such, by directly or indirectly exceeding the authorized access to customer accounts, wireless carriers such as T-Mobile may be liable under the Computer Fraud and Abuse Act (CFAA).

16. Unlike a direct hack of data where a company like T-Mobile plays a more passive role,[7] SIM-swaps are ultimately actualized by the wireless carrier itself. It is T-Mobile, in this case,

---

[6] A SIM ("subscriber identity module") card is a small, removable chip that allows a cell phone to communicate with the wireless carrier and to know which subscriber is associated with that phone. The SIM card associated with a wireless phone can be changed, allowing customers to move their wireless number from one cell phone to another and to continue accessing their carrier network when they switch cell phones. The wireless carrier must effectuate the SIM card reassignment.

[7] Of course, T-Mobile's security protocols have been proven to be extremely vulnerable to these sorts of hacks, as well, having admitted to multiple hacks of customer data over the past several years. Most recently, THE WALL STREET JOURNAL reported August 27, 2021 about the hack of T-Mobile's servers in Washington that exposed data on 50 million T-Mobile customers. *See* "*T-Mobile Hacker Who Stole Data on 50 Million Customers: 'Their Security is Awful*.'" (Aug. 27, 2021) (available at https://www.wsj.com/articles/t-

that effectuates the SIM card change. This action remains operative and in force when the victim's phone activity is used to hack other online accounts, extort the victim, or cause other foreseeable injuries, such as the one suffered by Plaintiff here.[8]

17. Once the third-party has access to the legitimate user's SIM-card data, it can seamlessly impersonate the legitimate wireless customer.

18. A common target of SIM-swapping and account takeover fraud are individuals known to, or expected to, hold large quantities of cryptocurrency as account information is often contained on users' cellular phones, allowing criminals to transfer the legitimate user's cryptocurrency to an account the criminal controls.

19. Particularly egregious is that T-Mobile customers report that they have been the subject of successful SIM-swap attacks on multiple occasions, even after T-Mobile has allegedly placed additional safeguards on previously hacked accounts.

20. SIM-swapping is not a new unforeseeable phenomenon but, instead, has been known to the wireless telephone industry for years and widely discussed by federal agencies since at least 2016.

---

mobile-hacker-who-stole-data-on-50-million-customers-their-security-is-awful-11629985105) (last accessed May 15, 2022).

[8] Wireless carriers such as T-Mobile have superior knowledge of their own and their customers' experience with SIM-swap attacks and can foresee identity theft and criminal impersonation of their customers following their effectuating of the SIM change. That a criminal may act as an intervening agent does not break the sequence of causation where T-Mobile had reasonable ground to anticipate such injuries to third-parties such as Plaintiff.

21. In June 2016, the FTC's Chief Technologist, herself the victim of an account takeover, recounted her experience and offered advice to wireless carriers to help consumers avoid these takeover attacks, stating:

> The mobile carriers are in a better position than their customers to prevent identity theft through mobile account hijacking and fraudulent new accounts. In fact, many of them are obligated to comply with the Red Flags Rule, which, among other things, requires them to have a written identity theft prevention program.
>
> Carriers should adopt a multi-level approach to authenticating both existing and new customers and require their own employees as well as third-party retailers to use it for all transactions …
>
> [M]obile carriers and third-party retailers need to be vigilant in their authentication practices to avoid putting their customers at risk of major financial loss and having email, social network, and other accounts compromised.[9]

22. Attention in the media and by government regulators, however, did not ensure that wireless carriers like T-Mobile took security seriously enough to prevent account takeover accounts and SIM-swapping schemes from increasing or, worse, to convince themselves, company-wide, to stop engaging in practices that were clearly violative of federal law.

23. An empirical study conducted by researchers at Princeton University in early 2020, the results of which were aware to T-Mobile prior to publication, concluded that they "identified

[9] "*Your Mobile Phone Account Could be Hijacked by an Identity Thief*," L. Cranor, Tech@FTC blog (June 7, 2016); Ms. Cranor also detailed her concerns about SIM-swapping in her reply comments before the Federal Communications Commission in July 2016 (In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunication Services; WC Docket No. 16-106; July 6, 2016).

weak authentication schemes and flawed policies" at several major wireless carriers in the United States, including T-Mobile.[10]

24. The researchers also concluded that "these flaws enable straightforward SIM swap attacks."[11]

25. One particularly weak form of customer authentication used by T-Mobile – the use of recent call logs – was identified as a "severe vulnerability," allowing criminals to authenticate a legitimate account by using information that can be manipulated without authentication.[12]

26. Indeed, when notified by the researchers of this "severe vulnerability," T-Mobile indicated that it would discontinue the use of call log verification in its customer authentication process in January 2020.

27. But, this is just the latest "vulnerability" that has been called out in T-Mobile's customer authentication process which, when flawed, enables criminals to easily secure access to the personal information of legitimate customers.

28. In May 2018, a popular information security blog, Krebs on Security, detailed several failures by T-Mobile to keep its customers' data secure, including failing to supervise its employees (one of whom perpetuated the account takeover scheme with knowledge of T-

[10] "*An Empirical Study of Wireless Carrier Authentication for SIM Swaps*," K. Lee, et al., Dept. of Comp. Sci. and Ctr. for Info. Tech. Policy, Princeton University (Jan. 10, 2020), at p. 10; *see also* p. 2 (discussing T-Mobile's discontinuation of call log verification based on the study's research in January 2020).

[11] Id.

[12] Id. at p. 6.

Mobile's vulnerable internal systems) and failing to send legitimate customers notice to their personal e-mail when a SIM-swap occurs.[13]

29. The article continued, "[T-Mobile] also acknowledged that it does not currently send customers an email to the email address on file when SIM swaps take place. A T-Mobile spokesperson said the company was considering changing the current policy, which sends the customer a text message to alert them about the SIM swap [to the phone number that is now in the criminal third-party's control]." As the author concluded with regard to sending a text to the hijacked phone number, "obviously that does not help someone who is the target of a SIM swap."[14]

30. As with the phone log verification vulnerability identified by Princeton researchers later, T-Mobile had already demonstrated a knowledge of multiple weaknesses in its internal processes and procedures to authenticate legitimate customers, admitting that such weaknesses must be eliminated, and such practices discontinued.

31. When Twitter CEO Jack Dorsey became the victim of a SIM-swap attack in 2019, the issue took on an even higher profile, with outlets including the NEW YORK TIMES and CNBC running lengthy articles on the topic, often including quotes from T-Mobile spokespersons.[15]

---

[13] "*T-Mobile Employee Made Unauthorized 'SIM Swap' to Steal Instagram Account*," B. Krebs, Krebs on Security (May 18, 2018).

[14] Id.

[15] "*Hackers Hit Twitter C.E.O. in a 'SIM Swap.' You're at Risk, Too*," N. Popper, NEW YORK TIMES (Sept. 5, 2019) (quoting a security expert who stated "SIM swapping is proliferating, and it's going to keep proliferating until companies deal with this. This is a known issue at this point. There is not really any excuse."); *see also* "*Here's How the Recent Twitter Attacks Happened and Why They're Becoming More Common*," A. Palmer, CNBC (noting that "As SIM hacks continue to rise, security advocates have called for carriers to do more

32. In February 2020, the FCC issued a "Notice of Apparent Liability for Forfeiture and Admonishment" against T-Mobile for apparently violating sections of the FCA governing the privacy of consumer information by disclosing such information to third-parties who were not authorized to receive it, finding, "even after highly publicized incidents put [T-Mobile] on notice that its safeguards for protecting [customer information] were inadequate, T-Mobile apparently continued sell access to its [customer information] for the better part of a year without putting in place reasonable safeguards – leaving its customers' data at unreasonable risk of unauthorized disclosure."[16]

33. In proposing a penalty of $91,630,000.00 against T-Mobile, the FCC concluded its decision by stating:

> Going forward, Americans must be able to place trust in their wireless carriers. I understand that operating businesses at the enormous scale of these companies means relying on third parties for certain services. But these carriers know that the services they offer create risks for users: unauthorized location tracking, SIM hijacking, and billing scams to name just [a] few. Carriers must take responsibility for those people they allow into their operations.[17]

to thwart the issue.") (available at https://www.cnbc.com/2019/09/06/hack-of-jack-dorseys-twitter-account-highlights-sim-swapping-threat.html) (last accessed Jan. 27, 2021).

[16] In the Matter of T-Mobile USA, Inc., File No. EB-TCD-18-00027702 (Feb. 28, 2020).

[17] Id. at p. 43.

34. In September 2021, the FCC began formal rule-making to combat SIM-swap attacks by requiring carriers to adopt certain secure methods of authenticating a customer before making a SIM change to a new device or carrier.[18]

35. In support of the proposed rule-making, FCC Commissioner Geoffrey Starks issued a statement dated September 30, 2021 which identified the danger SIM-swapping creates in situations exactly the same as this case, stating, "The scammer can then take control of the [customer data] associated with the victim's account, leverage that control to access bank accounts and other private information, and *impersonate the victim* in other harmful ways."[19]

36. Despite the massive amounts of media, governmental, and academic focus on the issue of SIM-swapping and the internal vulnerabilities of wireless carrier systems, T-Mobile has been unable or unwilling to institute the practices, procedures, and safeguards necessary to protect its customers' data from account takeover and SIM-swap attacks.[20]

37. Notwithstanding the publicity SIM-swapping attacks have generated across the world, as of February 8, 2022, and perhaps because of the failure of wireless carriers to stop the problem on their own, the Federal Bureau of Investigation (FBI) felt it necessary to issue an Alert

---

[18] Source: FCC News, "*FCC Begins Rulemaking to Combat Scams Used to Commandeer Consumers' Cell Phone Accounts – Seeks Input on Addressing SIM Swapping and Port-Out Fraud*" (Sept. 30, 2021).

[19] Available at https://www.fcc.gov/document/fcc-combating-scams-used-commandeer-consumers-cell-phone-accounts (last accessed May 15, 2022) (*emphasis added*).

[20] Setting aside the numerous instances of account takeover fraud, T-Mobile's track record on preventing data breaches of any kind is equally suspect, having announced at least four (4) separate data breaches in the last three (3) years, affecting millions of customers. When coupled with its merger partner, Sprint, the number of breaches is six (6) in the same time period. *See* https://threatpost.com/t-mobile-another-data-breach/162703/ (last accessed May 15, 2022).

(I-020822-PSA) to mobile carriers and the public of the increasing frequency of SIM-swap complaints, rising from 320 complaints (2018-2020) to 1,611 complaints (2021 alone), involving more than $68 million in losses.[21]

38. As a regulated wireless carrier and without regard to public statements by any federal, state, or consumer protection agency, T-Mobile has a well-established duty – one which it freely acknowledges on its corporate website[22] – to protect the security and privacy of its customers' personal and financial information – referred to as CPNI in federal statutory language[23] – from unauthorized access, which compliance with Federal law T-Mobile is required to certify annually to the FCC.[24]

39. The FCA expressly restricts carriers like T-Mobile from unauthorized disclosure of CPNI.

40. T-Mobile negligently failed to prevent the unauthorized disclosure of CPNI in this case, causing Plaintiff to suffer hundreds of thousands of dollars in damage.

---

[21] Available at https://www.ic3.gov/Media/Y2022/PSA220208 (last accessed May 15, 2022). The Alert recommended mobile carriers take the following precautions:

- Educate employees and conduct training sessions on SIM swapping
- Carefully inspect incoming email addresses containing official correspondence for slight changes that can make fraudulent addresses appear legitimate and resemble actual clients' names
- Set strict security protocols enabling employees to effectively verify customer credentials before changing their numbers to a new device
- Authenticate calls from third party authorized retailers requesting customer information

[22] *See* https://www.t-mobile.com/privacy-center/education-and-resources/cpni (last accessed May 15, 2022).

[23] CPNI stands for Customer Proprietary Network Information.

[24] *See* https://www.t-mobile.com/privacy-center/education-and-resources/cpni (last accessed May 15, 2022).

41. Indeed, upon information and belief, it was not until December 2021 that T-Mobile, via an internal employee memorandum, notified its personnel that it disabled the "Manager Override" option in their customer support software and began to require two (2) employees to verify customer credentials before allow a SIM to be swapped or ported to a different carrier.[25]

42. Such a change, entirely within T-Mobile's control, could have and should have been implemented many years ago, and, if done, could have potentially avoided the alleged damages in this action.

43. Despite the obvious nature of the change and the amount of publicity around the issue, T-Mobile nonetheless negligently failed to implement appropriate safeguards, failed to appropriately train T-Mobile personnel, and failed to prevent SIM-swaps such as the one at issue in this action.

THE SIM-SWAP AT ISSUE

44. At the time of the SIM-swap at issue, Brandon Buchanan ("**Buchanan**") was the co-founder and managing partner of Iterative Capital ("**Iterative**"), a hybrid investment fund focused on cryptocurrency trading and seed-stage venture investments.

45. Upon information and belief, Buchanan had been a customer of T-Mobile since 2016.

[25] See "*SIM Swaps are Finally a Bit More Secure on T-Mobile*;" https://tmo.report/2021/12/sim-swaps-are-finally-a-bit-more-secure-on-t-mobile/ (last accessed May 15, 2022).

46. Upon information and belief, in 2018, Buchanan was the victim of a prior SIM-swap attack while still a customer of T-Mobile.

47. Upon information and belief, following that attack and because his business involved cryptocurrency trading, Buchan requested additional protections be added to his T-Mobile account.

48. Upon information and belief, T-Mobile agreed to Buchanan's request and added security measures that prohibited the porting (i.e., transferring) of Buchanan's phone number and SIM data to any new device unless: (1) Buchanan appeared in person; and (2) he provided a secret Personal Identification Number (PIN).

49. Upon information and belief, Buchanan paid an additional monthly fee to add the "Protection 360 Tier 5" service to his account – a service advertised by T-Mobile as including "ID theft protection."

50. Upon information and belief, in reliance on the additional security measures put in place by T-Mobile, Buchanan continued using T-Mobile's wireless services.

51. In May 2020, Buchanan was still a wireless customer of T-Mobile.

52. In the days leading up to May 17, 2020, despite the additional protections placed on his T-Mobile account in the wake of his 2018 SIM-swap attack, Buchanan's suffered another SIM-swap attack when third parties were able to access and, indeed, hijack Buchanan's SIM data from T-Mobile, granting them full access to Buchanan's CPNI and allowing the third parties to impersonate Buchanan in online forums and applications.

53. T-Mobile customers like Buchanan, who was heavily involved in cryptocurrency trading, are particularly susceptible to the attention of hackers in account takeover and SIM-swap attacks.

54. Upon information and belief, Buchanan never appeared in person to request his number be ported to a new device nor did he provide T-Mobile (or anyone else) the confidential PIN required to port his number.

55. Upon information and belief, in subsequent discussions with T-Mobile's customer service department, T-Mobile representatives informed Buchanan that the SIM-swap appeared to be an "inside job," i.e., the hack involved a T-Mobile employee.

56. Knowing that he had been previously been hacked and in spite of the additional measures put in place to avoid this very result, T-Mobile nevertheless allowed unauthorized third parties other than Buchanan access to Buchanan's SIM data in violation of federal and state law.

57. Plaintiff is a customer of Iterative.

58. Iterative administered a cryptocurrency exchange where its customers could buy and sell cryptocurrencies, including Bitcoin.

59. Plaintiff performed several successful transactions with Iterative to purchase Bitcoin in the months leading up to May 2020.

60. The transactions were coordinated through a mobile application ("app") called Telegram, an encrypted cloud-based instant messaging software.

61. As of January 2022, Telegram had an estimated 550 million monthly active users worldwide, with accounts tied to cellular telephone numbers which are verified by text message to those telephone numbers.

62. If an unauthorized third-party gains access to a Telegram account holder's SIM data, it can easily access that user's Telegram account and hijack that user's identity in messages with other Telegram account users.

63. Plaintiff maintained a Telegram account to perform the cryptocurrency transactions with Iterative.

64. Buchanan was a member of Telegram group chat room used by Plaintiff to conduct transactions with Iterative.

65. Plaintiff was aware Buchanan was a member of the Telegram group chat room used to conduct the cryptocurrency trades.

66. Plaintiff knew Buchanan to be an officer and principal of Iterative.

67. Another member of Iterative, Wei Lin ("**Wei**"), was also a member of the same Telegram group chat room used by Plaintiff and Iterative to conduct the cryptocurrency exchange transactions.

68. Plaintiff knew Wei to be a representative of Iterative.

69. Plaintiff was aware Wei was a member of the Telegram group chat room used to conduct the cryptocurrency trades.

70. After securing access to Buchanan's data from T-Mobile, the hackers compromised Buchanan's Telegram account.

71. After securing access to Buchanan's data from T-Mobile, the hackers impersonated Buchanan by sending a Telegram message to Plaintiff, inquiring whether Plaintiff wanted to sell any Bitcoin for an Iterative client at a premium (i.e., above market value) on or about May 17, 2020 at 7:31 p.m.

72. When Plaintiff inquired further, the hackers stated under the Telegram username "Brandon B. [Iterative Capital]" that "I'm a partner & Co-founder at Iterative capital, I believe you've done a buy with Wei before, check our Groups in common."

73. Believing the proposed transaction to be a legitimate trade with a principal of Iterative, Plaintiff sent fifteen (15) Bitcoin to a digital wallet he believed to be controlled by Buchanan and/or Iterative, expecting U.S. dollars in return to an account controlled by Plaintiff.

74. Plaintiff did not receive any money in return for the fifteen (15) Bitcoin he sent via the Telegram app to the party he thought was Buchanan.

75. The record of the May 17, 2020 transaction and communications between Plaintiff and the third parties Plaintiff believed to be Buchanan were deleted thereafter from the Telegram app.

76. On May 19, 2020, Buchanan sent an email to Iterative's exchange clients informing them that several of his accounts were compromised "as a result of a SIM-swap attack that enabled a hacker to assume my identity" and to make trades on behalf of Iterative.

77. Buchanan alerted local law enforcement (New York Police Department) authorities, as well as the Federal Bureau of Investigation (FBI).

78. The investigation into the identity of the third parties who gained access to Buchanan's SIM data from T-Mobile is ongoing.

79. Plaintiff, likewise, filed complaints with the same law enforcement agencies.

80. Upon information and belief, Buchanan attempted to intercede directly with T-Mobile to obtain a refund on behalf of Plaintiff.

81. Upon information and belief, T-Mobile did not offer to compensate Buchanan or Plaintiff in any way, despite the clear violation of federal and state law and its negligence in securing Buchanan's CPNI, which violations of law and duty cost Plaintiff hundreds of thousands of dollars in losses.

82. Upon information and belief, T-Mobile, despite a legal obligation to do so, abjectly failed in its duty to safeguard its customers' personal and financial information by providing unauthorized access to Buchanan's CPNI.

83. Upon information and belief, T-Mobile failed to implement and/or maintain security policies and procedures sufficient to protect the unauthorized access to Buchanan's CPNI.

84. Upon information and belief, T-Mobile failed to properly train and supervise its employees to prevent the unauthorized access to Buchanan's CPNI.

85. Upon information and belief, T-Mobile failed to implement the additional security measures added to Buchanan's account following his 2018 SIM-swap attack and allowed unauthorized access to Buchanan's CPNI again in 2020.

86. Upon information and belief, T-Mobile could have reasonably foreseen the consequences of failing in its duty to implement, maintain, and execute sufficient security policies and practices to protect the unauthorized access to customer data, including that of Buchanan.

87. Upon information and belief, T-Mobile's systems, policies, and procedures allow its officers, agents, and employees to exceed the authorized access to its customer accounts without justification in violation of, among other statutes, the CFAA.

88. T-Mobile's actions and inaction demonstrate a reckless disregard for the rights of its customers and those with whom its customers deal (i.e., foreseeable victims).

89. T-Mobile's actions and inaction demonstrate a reckless disregard for its obligations, responsibilities, and duties under the law.

90. But for T-Mobile's reckless disregard of its obligations, Plaintiff would not have been damaged.

91. The damage suffered by Plaintiff is fairly traceable to the wrongful conduct of T-Mobile in allowing the unauthorized access to Buchanan's wireless account.

JURISDICTION AND VENUE

92. This Court has jurisdiction over this matter under 28 U.S.C. §1331 as this case arises under the Court's federal question jurisdiction pursuant to the Federal Communications Act ("**FCA**").

93. This Court has jurisdiction over this matter under 18 U.S.C. §1030(g) as this case arises under the Court's federal question jurisdiction and monetary threshold requirements pursuant to the Computer Fraud and Abuse Act ("**CFAA**").

94. Pursuant to the Court's supplemental jurisdiction under 28 U.S.C. §1367, it may entertain the state law claims as they are derived from a common nucleus of operative facts.

95. Further, the Court has jurisdiction under 28 U.S.C. §1332 in that the amount in controversy exceeds $75,000.00 and Plaintiff and Defendant are citizens of different states.

Plaintiff is a resident of the State of California, and Defendant is a Delaware corporation with a principal place of business in the State of Washington.

96. Venue is proper in this Court under 28 U.S.C. §1391(b)(2), §1391(b)(3), §1391(c)(2), and §1391(d) as a substantial part of the events or omissions giving rise to this complaint occurred in this District. At the time of the occurrence, Buchanan was a resident of the State of New York, Iterative maintained its principal place of business in the State of New York, and Buchanan utilized the T-Mobile wireless services in the State of New York, including the use of a New York area code.

97. Upon information and belief, as a resident of New York, Buchanan contracted with T-Mobile to provide wireless carrier services in the State of New York, including the data security protections against unauthorized disclosure by T-Mobile of Buchanan's data, as required by federal law. As such, T-Mobile's failure to protect Buchanan's CPNI against unauthorized access, causing Plaintiff damage, is central to the claims of this complaint.

98. As a customer of Iterative, a New York-based company, Plaintiff conducted trades through the platforms maintained by Iterative and, additionally, signing a contract governing such trades.

99. The investigation into the fraudulent trade is currently being led by the New York Police Department's Financial Crimes Task Force (Det. A. Napoli) in conjunction with the U.S. Department of Homeland Security, Dark Web & Crypto Currency Group – TFO.

100. Upon information and belief, the necessary witnesses, including Buchanan, Wei, and Iterative, are resident in the State of New York.

PARTIES

101. Plaintiff is a citizen of the United States and a resident of the State of California.

102. T-Mobile is a corporation formed under the laws of the State of Delaware and serves as the American operating company of T-Mobile International AG. & Co., a corporation based in Germany. T-Mobile maintains its headquarters and principal place of business in Bellevue, Washington.

103. The practices and acts of T-Mobile, as alleged herein, are "charges, practices, classifications, and regulations" by a common carrier engaged in interstate commerce as set forth in the FCA.

FACTS AND ALLEGATIONS COMMON TO ALL CLAIMS

104. T-Mobile markets and sells wireless cellular phone service through standardized wireless service plans via various retail locations, online sales, and over the telephone.

105. T-Mobile maintains accounts for its wireless customers, enabling them to access information about the services they purchase from T-Mobile.

106. It is widely recognized and has been widely publicized that mishandling of customer wireless accounts, including but not limited to allowing unauthorized access, can facilitate identity theft and related consumer harm.

107. Instances of mishandling of customer account information have occurred on numerous occasions at T-Mobile.

108. T-Mobile's Privacy Policy states in 2022, in pertinent part: "We use administrative, technical, contractual, and physical safeguards designed to protect your data. For example, when you contact us by phone or visit us in our stores, we have procedures in place to make sure that only the primary account holder or authorized users have access. We can't guarantee our safeguards will prevent every unauthorized attempt to access, use, or disclose personal data. Be sure to use a strong password to access your information and not one you use for other services. You should also use multi-factor authentication where possible."

109. As above, the Privacy Policy stated something considerably different when the events at issue occurred.[26]

110. T-Mobile's sales and marketing materials has stated, *inter alia*, "We have implemented various policies and measures to ensure that our interactions are with you or those you authorize to interact with us on your behalf – and not with others pretending to be you or claiming a right to access your information."

111. T-Mobile's sales and marketing materials have also stated that, unless T-Mobile can verify the caller's identity through certain personal information or a PIN requested by the customer, T-Mobile's policy is not to release any account specific information.

[26] In January 2021, for example, the T-Mobile Privacy Policy stated that is used a "variety of administrative, technical, procedural, contractual, and physical security measures" to protect customer data against "accidental, unlawful, or unauthorized destruction, loss, alteration, access, disclosure, or use while it is under our control" and that it maintained "authentication procedures when [customers] contact us by phone or in retail locations to help ensure that access is provided only to the primary account holder or authorized users of the account." The latter, of course, is no longer in the Privacy Policy, and the former has been modified to eliminate any reference to "procedural" security measures. Clearly, T-Mobile has made numerous changes to such policy in response to the potential liability associated with its many data breaches and the attendant publicity of takeover schemes like SIM-swaps.

112. Despite these statements and other similar statements and promises, T-Mobile failed to provide reasonable and appropriate security to prevent unauthorized access to customer accounts.

113. Because of the inadequate procedures implemented by T-Mobile, unauthorized persons, including T-Mobile's own officers, agents, and employees, acting without customer permission, could authenticate, access, and make changes to information to customer information.

114. Given the numerous breaches of its security procedures and the hundreds of cases of SIM-swap account takeover, the statements made by T-Mobile in its privacy and sales material are clearly deceptive and designed to deceive customers and those who deal with T-Mobile customers into believing its customer data has not been compromised.

115. Indeed, upon information and belief, it could very well be that every single T-Mobile customer has been subject to having his or her data compromised at some point in time, given the numerous data hacks admitted to by T-Mobile and its affiliated entities in the last four (4) years.

116. Nevertheless, T-Mobile failed to disclose or made deceptive statements designed to cover up for the fact that its security procedures can, did, and have fallen short of its expressed and implied representations and promises.

117. Such failures leading to unauthorized access of customer information and the likelihood that such unauthorized access could be used to dupe third-parties were entirely foreseeable by T-Mobile.

118. Upon information and belief, Buchanan entered into a contract with T-Mobile for wireless cellular service in or about 2016.

119. Upon information and belief, in 2018, Buchanan was the subject of a SIM-swap attack.

120. Thereafter, upon information and belief, Buchanan requested additional account protection on his T-Mobile account to prevent further SIM-swap attacks, including requiring a personal appearance and a secret PIN before his SIM data could be transferred to another device.

121. Upon information and belief, T-Mobile agreed to the additional account protections and, indeed, charged Buchanan additional fees for such protection.

122. On or about May 17, 2020, T-Mobile again allowed an unauthorized person to access Buchanan's T-Mobile account.

123. Subsequently, the unauthorized person was able to gain access to Buchanan's phone-based applications, including Telegram.

124. The unauthorized person was able to impersonate Buchanan and engage in transactions with third parties, including Plaintiff.

125. Plaintiff lost fifteen (15) Bitcoin because of his belief he was doing business with Buchanan, a loss in excess of $750,000.00.

126. Had T-Mobile not allowed the unauthorized access to Buchanan's account, Plaintiff would not have suffered his loss.

127. T-Mobile, because of its inadequate procedures, practices, and regulations, engaged in practices which, taken together, failed to provide reasonable, appropriate, and sufficient security to prevent unauthorized access to its customers' wireless accounts, allowing

unauthorized persons to be authenticated, and granting access to sensitive customer account information.

128. In particular, T-Mobile failed to establish and implement reasonable policies, procedures, and safeguards governing the creation, access, and authentication of user credentials to access customer accounts, creating an unreasonable risk of unauthorized access.

129. As such, in violation of federal law, T-Mobile has failed to ensure that only authorized persons have access to customer account data and that customer CPNI is secure.

130. Among other things, T-Mobile:

a. Failed to establish and enforce rules and procedures sufficient to ensure only authorized persons have access to T-Mobile customer accounts;

b. Failed to establish appropriate rules, policies, and procedures for the supervision and control of its officers, agents, and employees;

c. Failed to establish and enforce rules and procedures, or provide adequate supervisions or training sufficient to ensure that its employees and agents follow such rules and procedures, to restrict access by unauthorized persons;

d. Failed to establish and enforce rules and procedures to ensure T-Mobile's employees and agents adhere to the security instructions of customers with regard to accessing customer accounts;

e. Failed to adequately safeguard and protect its customers' wireless accounts;

f. Permitted the sharing of and access to user credentials among T-Mobile's agents or employees without a pending request from the customer, reducing the likely detection of and accountability for unauthorized access;

g. Failed to appropriately supervise employees and agents who granted unauthorized access to customer accounts;

h. Failed to adequately train and supervise its employees, officers, and agents to prevent the unauthorized access to customer accounts;

i. Failed to prevent the ability of employees, officers, and agents to access and make changes to customer accounts without specific customer authorization;

j. Allowed porting out of cell phone numbers without properly confirming that the request was coming from legitimate customers;

k. Lacked proper monitoring solutions and therefore failed to monitor its systems for the presence of unauthorized access in a manner that would allow T-Mobile to detect intrusions, breaches of security, and unauthorized access to customer information;

l. Failed to implement and maintain readily available best practices to safeguard customer information; and

m. Failed to implement and maintain internal controls to help protect against account takeovers and SIM-swapping by unauthorized persons.

131. Due to the inadequate security measures, policies, and safeguards employed by T-Mobile, it created an unreasonable risk of unauthorized access to the accounts of its customers, including that of Buchanan.

132. Upon information and belief, T-Mobile has been long aware of its inadequate security measures, policies, and safeguards and, nevertheless, induced customers into believing that its systems were secure and compliant with applicable law.

133. T-Mobile, despite knowing the risks associated with unauthorized access to customer accounts, failed to utilize reasonable and available methods to prevent or limit such unauthorized access.

134. In sum, T-Mobile's security measures were entirely inadequate to prevent the foreseeable damage caused to Plaintiff.

135. T-Mobile failed in its duty to protect and safeguard customer information and data pursuant to federal law.

136. Had T-Mobile implemented appropriate and reasonable security measures, Plaintiff would not have been damaged.

AS AND FOR A FIRST CAUSE OF ACTION

(Violations of the Federal Communications Act)

137. Plaintiff incorporates herein by reference the claims and allegations set forth above, inclusive, as fully set forth herein.

138. The FCA regulates interstate telecommunications carriers, including T-Mobile.

139. T-Mobile is a "common carrier" engaged in interstate commerce by wire for the purpose of furnishing communication services within the meaning of Section 201(a) of the FCA.

140. As a common carrier, T-Mobile is subject to the substantive requirements of Sections 201 through 222 of the FCA.

141. Under Section 201(b) of the FCA, common carriers may implement only those practices, classifications, and regulations that are "just and reasonable" and practices that are "unjust or unreasonable" are unlawful.

142. Section 206 of the FCA provides:

> In case any common carrier shall do, or cause or permit to be done, any act, matter, or thing in this chapter prohibited or declared to be unlawful, or shall omit to do any act, matter, or thing in this chapter required to be done, such common carrier shall be liable to the person or persons injured thereby for the full amount of damages sustained in consequence of any such violation of the provisions of this chapter, together with a reasonable counsel or attorney's fee, to be fixed by the court in every case of recovery, which attorney's fee shall be taxed and collected as part of the costs in the case.

143. T-Mobile's conduct, as alleged herein, constitutes a knowing violation of Section 201(b) of the FCA.

144. T-Mobile is also liable for the acts, omissions, and/or failures, as alleged herein, of any of its officers, employees, agents, or any other person acting for on behalf of T-Mobile.

145. Section 222 of the FCA requires telecommunications carriers, including T-Mobile, to "protect the confidentiality of proprietary information" of, *inter alia*, customers.

146. T-Mobile violated its duty under Section 222 of the FCA by failing to protect the confidentiality of the proprietary information of Buchanan by using, disclosing, or permitting

access to Buchanan's CPNI without the consent, notice, and/or legal authorization of Buchanan as required by the FCA.

147. T-Mobile's violations under Section 222 allowed unauthorized parties to impersonate Buchanan in transactions with other parties, including Plaintiff.

148. T-Mobile violated Section 222 by allowing an unauthorized party to access Buchanan's CPNI, resulting in the theft by that party or others associated with that party of fifteen (15) Bitcoin belonging to Plaintiff, valued in excess of $750,000.00.

149. T-Mobile's conduct as alleged herein constitutes a knowing violation of Section 222 of the FCA.

150. As a direct consequence of T-Mobile's violations of the FCA, Plaintiff has been damaged in an amount to be proven at trial but, upon information and belief, exceeds $750,000.00 plus fees and costs, including reasonable attorneys' fees.

AS AND FOR A SECOND CAUSE OF ACTION

(Violations of the Computer Fraud and Abuse Act)

151. Plaintiff incorporates herein by reference the claims and allegations set forth above, inclusive, as fully set forth herein.

152. The CFAA governs those who intentionally access computers without authorization or who intentionally exceed authorized access[27] and as a result of such conduct, cause damage and loss.

153. As alleged herein, a SIM-swap attack requires the intentional access to customer computer data by T-Mobile which exceeds its authority, and which conduct causes damage and loss.

154. As such, T-Mobile is subject to the provisions of the CFAA.

155. T-Mobile's conduct, as alleged herein, constitutes a knowing violation of the CFAA.

156. T-Mobile is also liable for the acts, omissions, and/or failures, as alleged herein, of any of its officers, employees, agents, or any other person acting for on behalf of T-Mobile.

157. T-Mobile violated its duty under the CFAA by exceeding its authority to access the computer data and breach the confidentiality of the proprietary information of Buchanan by using, disclosing, or permitting access to Buchanan's CPNI without the consent, notice, and/or legal authorization of Buchanan as required by the CFAA.

158. Section 1030(g) of the CFAA provides, in pertinent part:

> Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages. No

[27] As set forth in the CFAA, the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser [*sic*] is not entitled so to obtain or alter. 18 U.S.C. §1030(e)(6).

> action may be brough under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage….

159. Plaintiff alleges he has suffered damages which exceed the threshold of $5,000.00 as required by Section 1030(c)(4)(A)(i)(I) of the CFAA.

160. Plaintiff alleges T-Mobile's unlawful conduct has caused damage which exceeds approximately $750,000.00.

161. Plaintiff has brought this claim within two (2) years of the date of discovery of the damage pursuant to Section 1030(g) of the CFAA.

162. Plaintiff discovered the damage on or about May 19, 2020.

163. Upon information and belief, T-Mobile's conduct as alleged herein constitutes a violation of Section (a)(5)(A) of the CFAA.

164. Upon information and belief, T-Mobile's conduct as alleged herein may constitute a reckless violation of Section (a)(5)(B) of the CFAA.

165. Upon information and belief, T-Mobile's conduct as alleged herein may constitute an intentional violation of Section (a)(5)(C) of the CFAA.

166. As a direct consequence of T-Mobile's violations of the CFAA, Plaintiff has been damaged in an amount to be proven at trial but, upon information and belief, exceeds $750,000.00 plus fees and costs, including reasonable attorneys' fees.

AS AND FOR A THIRD CAUSE OF ACTION

(Negligence)

167. Plaintiff incorporates herein by reference the claims and allegations set forth above, inclusive, as fully set forth herein.

168. T-Mobile owes a duty of care to its customers to ensure the privacy and confidentiality of CPNI during its provision of wireless carrier services, as required by both federal and state law.

169. T-Mobile also owes a duty of care to foreseeable victims who transact business with legitimate T-Mobile customers or those who they have reason to believe to be are legitimate T-Mobile customers.

170. T-Mobile was aware of the possibility of SIM-swap attacks and, despite placing additional security measures on Buchanan's account, it nevertheless failed to prevent a second SIM-swap attack on Buchanan's account.

171. By allowing unauthorized access to the personal and confidential information of legitimate T-Mobile customers, T-Mobile breached its duty of care to its customers and to reasonably foreseeable victims, including Plaintiff.

172. But for the inadequate security protocols, practices, and procedures employed by T-Mobile in protecting customer data, including Buchanan's private and confidential information, Plaintiff would not have suffered damage.

173. Plaintiff has been damaged in an amount equal to fifteen (15) Bitcoin, which, upon information and belief, is valued in excess of $750,000.00.

AS AND FOR A FOURTH CAUSE OF ACTION

(Violations of the New York Consumer Protection Act – N.Y. Gen. Bus. L. § 349)

174. Plaintiff incorporates herein by reference the claims and allegations set forth above, inclusive, as fully set forth herein.

175. NEW YORK GENERAL BUSINESS LAW (GBL), §349(a) provides, in pertinent part, that "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful."

176. GBL §349(h) provides, in pertinent part, that "any person who has been injured by reason of any violation of this section may bring an action in his own name to enjoin such unlawful act or practice, an action to recover his actual damages …" including "reasonable attorney's fees."

177. T-Mobile's acts as alleged herein, including but not limited to its sales and marketing representations about its level of data security and confidentiality and the measures it employs to keep customer data secure, induced customers to trade with T-Mobile notwithstanding T-Mobile's knowledge that its security protocols and procedures were inadequate to prevent unauthorized access to customer CPNI.

178. T-Mobile's acts as alleged herein violated federal and state law, particularly those related to the safeguarding of customer CPNI and such violations are deemed to be violations of GBL §349.

179. Given T-Mobile's superior knowledge of its systems, procedures, and practices, coupled with its experience with past breaches of data security, Plaintiff was a foreseeable victim of the violative acts of T-Mobile.

180. Given T-Mobile's knowledge of the additional security measures in place on Buchanan's account and its prior allowance of a SIM-swap attack against Buchanan, Plaintiff was a foreseeable victim of the violative acts of T-Mobile

181. By allowing unauthorized access to Buchanan's confidential and proprietary information, T-Mobile facilitated and thereby assisted unauthorized third parties to prey upon innocent victims like Plaintiff.

182. Had T-Mobile not engaged in deceptive acts and practices, Plaintiff would not have been damaged.

183. Had T-Mobile accurately represented the nature of its security measures, or lack thereof, Plaintiff would not have conducted business with Buchanan and would not have been damaged by those who gained unauthorized access to Buchanan's CPNI from T-Mobile.

184. As a result of T-Mobile's deceptive acts and practices, as defined by federal and state law, Plaintiff suffered actual harm in an amount equal to fifteen (15) Bitcoin, valued in excess of $750,000.00.

185. As a result of T-Mobile's deceptive acts and practices, Plaintiff is entitled to actual and statutory damages, including reasonable attorneys' fees.

AS AND FOR A FIFTH CAUSE OF ACTION

(Negligent Hiring, Retention, and Supervision)

186. Plaintiff incorporates herein by reference the claims and allegations set forth above, inclusive, as fully set forth herein.

187. At all material times herein, T-Mobile's agents, officers, and employees, including those directly or indirectly responsible for or involved in allowing unauthorized access to Buchanan's confidential and proprietary account information, were under T-Mobile's direct supervision and control.

188. Upon information and belief, T-Mobile negligently hired, retained, controlled, trained, and supervised the officers, agents, and employees under its control, and knew or should have known that such officers, agents, and employees could allow unauthorized access to customer accounts, including that of Buchanan.

189. Upon information and belief, T-Mobile negligently failed to implement systems and procedures necessary to prevent its officers, agents, and employees from allowing unauthorized access to customer accounts, including that of Buchanan.

190. Upon information and belief, T-Mobile's negligent hiring, retention, control, training, and supervision allowed the unauthorized access to customer accounts resulting in damage to T-Mobile customers and foreseeable victims in the public at large, including Plaintiff.

191. Given T-Mobile's experience with account takeover and SIM-swap attacks, many of them assisted by the actions of its officers, agents, and/or employees, T-Mobile's failure to exercise reasonable care in supervising and controlling its officers, agents, and employees was a breach of its duty to its customers and to those potential victims, including Plaintiff, with whom they interacted.

192. T-Mobile's duty to its customer and foreseeable victims to protect its customer data from unauthorized access is required by federal and state law.

193. It was entirely foreseeable to T-Mobile that unauthorized persons would attempt to gain unauthorized access to T-Mobile customer data and, despite this, T-Mobile failed to implement sufficient safeguards and procedures to prevent its officers, agents, and employees from granting such unauthorized access.

194. Upon information and belief, T-Mobile engaged in the acts alleged herein and/or condoned, permitted, authorized, and/or ratified the conduct of its officers, agents, and employees.

195. As a direct consequence of T-Mobile's negligent hiring, retention, control, and supervision of its officers, agents, and employees who allowed the unauthorized access to Buchanan's account, Plaintiff was damaged in an amount to be proved at trial, but, upon information and belief, an amount that exceeds $750,000.00

AS AND FOR A SIXTH CAUSE OF ACTION

(Gross Negligence)

196. Plaintiff incorporates herein by reference the claims and allegations set forth above, inclusive, as fully set forth herein.

197. T-Mobile, as required by federal and state law, owed Buchanan and foreseeable victims a duty to properly handle and safeguard Buchanan's CPNI and access to his account.

198. Under the FCA, T-Mobile was required to "do any act, matter, or thing in this chapter required to be done" to ensure its compliance with federal law and to protect the confidentiality of its customer account data, including that of Buchanan.

199. Upon information and belief, T-Mobile willfully disregarded and/or showed reckless indifference to its duties under federal and state law to T-Mobile customers and to foreseeable victims of T-Mobile's wrongful acts.

200. Having superior knowledge of prior account takeover attacks on T-Mobile customers' data and having the ability to employ internal systems, procedures, and safeguards to prevent such attacks, T-Mobile nevertheless failed to institute appropriate controls to prevent unauthorized access to customer accounts, utilized authentication systems it knew or should have known were vulnerable to account takeover attacks, willfully disregarded the best practices of the industry in failing to implement systems to thwart such attacks, and failed to appropriately hire, retain, supervise, train, and control those officers, agents, and employees who could grant unauthorized access to customer account data.

201. T-Mobile's policies, procedures, and safeguards were completely ineffective and inadequate to prevent the unauthorized access to its customers' data, notwithstanding the requirements of the CFAA.

202. T-Mobile's actions as alleged herein, in the face of an abundance of attention by the media and government regulators, evince a carelessness that can only be characterized as a complete disregard for the rights of its customers and the foreseeable victims of its inadequate data security measures.

203. T-Mobile's actions as alleged herein, in the face of a previous SIM-swap attack on Buchanan in 2018 and the implementation of enhanced security measures on Buchanan's account, completely and utterly failed to implement the necessary protocols and safeguards in blatant disregard its customers and the foreseeable victims of its inadequate data security measures.

204. As a consequence of T-Mobile's gross negligence, Plaintiff has been damaged in an amount to be proved at trial, but, upon information and belief, an amount that exceeds $750,000.00.

DEMAND FOR JURY TRIAL

Plaintiff respectfully demands a trial by jury for all issues set forth herein.

PRAYER FOR RELIEF

WHEREFORE Plaintiff prays for judgment against T-Mobile as follows:

1) Enter judgment for Plaintiff on all counts
2) Award compensatory damages to Plaintiff arising from T-Mobile's negligence;
3) Award punitive damages to Plaintiff due to the willfulness and gross negligence of T-Mobile's conduct;
4) Award statutory damages to Plaintiff for T-Mobile's FCA violations;
5) Award statutory damages to Plaintiff for T-Mobile's CFAA violations;
6) Award Plaintiff costs and reasonable attorneys' fees;
7) Award Plaintiff prejudgment interest; and
8) Award Plaintiff such other and further relief as this Court deems just, fair, and proper.

(signature page follows)

Dated: May 16, 2022

Wilson & Chan LLP

Jeffrey L. Wilson, Esq. (JW9819)
Henry C. Chan, Esq. (HC4160)
Attorneys for Plaintiff CALVIN CHENG
733 Third Avenue, 16th Floor
New York, NY 10017
jwilson@wilsonchanlaw.com
hchan@wilsonchanlaw.com
Tel. (646) 790-5848